IN THE CLAIMS

Please amend the claims as follows:

1. (currently amended) A method ~~for sharing the authorization to use specific resources among multiple devices (11,13), which resources are accessible via messages on which a secret key operation was applied with a predetermined secret master key (d) available at a master device (11), said method~~ comprising:
   - generating at a master device a first part and a second part of a predetermined secret master key, said predetermined secret master key being available at said master device and said first part and said second part being combinable to said secret master key~~splitting said secret master key (d) at said master device (11) into a first part (d_1) and a second part (d_2)~~, wherein resources are accessible via messages on which a secret key operation was applied with said secret master key and wherein said master device ~~(11)~~ is acting as a delegator of an ~~said~~ authorization to use said specific resources;
   - forwarding a piece of information to a slave device ~~(13)~~ acting as a delegatee of said authorization, which piece of information enables said slave device ~~(13)~~ to perform a partial secret key operation on messages ~~(m)~~ based on said first part ~~(d_1)~~ of said secret master key ~~(d)~~; and
   - forwarding said second part ~~(d_2)~~ of said secret master key ~~(d)~~ to a server ~~(12)~~ for enabling said server ~~(12)~~ to perform a partial secret key operation on messages ~~(m)~~ received from said slave device ~~(13)~~ based on said second part ~~(d_2)~~ of said secret master key ~~(d)~~.

2. (currently amended) A method according to claim 1, wherein a delegatee ~~(13)~~ to which said authorization was delegated is enabled to act as delegator for delegating said authorization to another slave devices ~~(23)~~ acting as delegatee, said method comprising for said further delegation:

- generating at said delegator a further first part and another part of said first part of said secret master key, which can be generated at said delegator, said further first part and said other part being combinable to said first part of said secret master keysplitting a first part (d_1) of said secret master key (d) which can be generated at said delegator (13) into a further first part (d_{11}) of said secret master key (d) and another part (d'_{21});
- forwarding a piece of information to said delegatee (23), which piece of information enables said delegatee (23) to perform a partial secret key operation on messages (m) based on said further first part (d_{11});
- forwarding said other part (d'_{21}) of said first part (d_1) of said secret master key (d) to said server (12); and
- combining a second part (d_2) of said secret master key (d) available at said server (12) for said delegator (13) with said other part (d'_{21}) provided by said delegator (13) to a further second part (d_{21}) of said secret master key (d) for enabling said server (12) to perform a partial secret key operation on messages (m) received from said delegatee (23) based on said further second part (d_{21}) of said secret master key (d).

3. (currently amended) A method according to claim 1, wherein generating a first part and a second part of a predetermined secret master key said step of splitting a key (d,d_1) at a respective delegator (11,13) into two parts is preceded by: the steps of
   - generating a password verification value (b) at a respective delegatee (13,23) based on a password input by a user (15) of said delegatee (13,23) and on a first random number; and
   - providing said password verification value (b) to said delegator (11,13);

   wherein said respective first part (d_1,d_{11}) of said secret master key (d) is determined at said delegator (11,13) based on said password verification value (b) received from said delegatee (13,23) and on a second random number (v) and wherein said piece of information which is forwarded by said delegator (11,13) to said delegatee (13,23) comprises said second random number (v)

for enabling said delegatee ~~(13,23)~~ to generate said respective first part ~~(d_1,d_{11})~~ of said secret master key ~~(d)~~.

4. (currently amended) A method according to claim 1, wherein said delegator ~~(11,13)~~ determines a respective second part ~~(d_2,d'_{21})~~ of an available secret key ~~(d,d_1)~~ as the difference between said available secret key ~~(d,d_1)~~ and a randomly generated first part ~~(d_1,d_{11})~~ of said secret master key ~~(d)~~.

5. (currently amended) A method according to claim 1, wherein a delegator ~~(11,13)~~ provides in addition policy data to said server ~~(12)~~ restricting the bounds of the authorization that may be delegated to a delegatee ~~(13,23)~~.

6. (currently amended) A method according to claim 5, wherein said bounds comprise a delegation bound indicating the maximum number of allowed further delegations of said authorization by a respective delegatee ~~(13)~~ acting as a delegator for further delegatees ~~(23)~~.

7. (currently amended) A method according to claim 5, wherein said bounds are content bounds comprising at least one value which can be compared to the values of attributes in a message ~~(m)~~ on which a secret key operation is to be performed, said message ~~(m)~~ having a pre-defined structure including said attributes.

8. (currently amended) A method according to claim 1, wherein said delegator ~~(11,13)~~ transmits a respective second part ~~(d_2,d'_{21})~~ of an available secret key ~~(d,d_1)~~ computed for a specific delegatee ~~(13,23)~~ directly to said server ~~(12)~~ once during an initialization process for a specific delegatee ~~(13,23)~~.

9. (currently amended) A method according to claim 1, wherein said delegator ~~(11,13)~~ transmits a respective second part ~~(d_2,d'_{21})~~ of an available secret key ~~(d,d_1)~~ computed for a specific delegatee ~~(13,23)~~ directly to said server ~~(12)~~

upon a request by said server ~~(12)~~ each time said specific delegatee ~~(13,23)~~ requests a partial secret key operation on a message ~~(m)~~.

10. (currently amended) A method according to claim 1, wherein said delegator ~~(11,13)~~ transmits a respective second part ~~(d_2,d'_{21})~~ of an available secret key ~~(d,d_1)~~ computed for a specific delegatee ~~(13,23)~~ to said server via said specific delegatee ~~(13,23)~~ once during an initialisation process.

11. (currently amended) A method according to claim 1, wherein said delegator ~~(11,13)~~ transmits a respective second part ~~(d_2,d'_{21})~~ of an available secret key ~~(d,d_1)~~ computed for a specific delegatee ~~(13,23)~~ to said server ~~(12)~~ via said specific delegatee ~~(13,23)~~, said specific delegatee ~~(13,23)~~ forwarding said respective second part ~~(d_2,d'_{21})~~ to said server ~~(12)~~ each time it requests a partial secret key operation on a message ~~(m)~~ from said server ~~(12)~~.

12. (currently amended) A method according to claim 1, wherein a confidential channel can be established between a respective delegator ~~(11,13)~~ and a respective delegatee ~~(13,23)~~ for securely transmitting confidential information between said delegator ~~(11,13)~~ and said delegatee ~~(13,23)~~.

13. (currently amended) A method according to claim 1, wherein a security association is formed between a respective delegator ~~(11,13)~~ and said server ~~(12)~~ for securely transmitting confidential information between said delegator ~~(11,13)~~ to said server ~~(12)~~.

14. (currently amended) A method according to claim 13, wherein said security association is realized with a symmetric algorithm using cryptographic parameters ~~(K(ID),A(ID))~~ associated to said delegator ~~(11,13)~~, which cryptographic parameters ~~(K(ID),A(ID))~~ are available at said delegator ~~(13)~~ and at said server ~~(12)~~.

15. (currently amended) A method according to claim 1, wherein a security association is formed between a respective delegatee ~~(13,23)~~ and said server ~~(12)~~ for securely transmitting confidential information between said delegatee ~~(13,23)~~ and said server ~~(12)~~.

16. (currently amended) A method according to claim 15, wherein said security association is realized with a symmetric algorithm using cryptographic parameters ~~(K(ID),A(ID))~~ associated to said delegatee ~~(13)~~ and available at said delegatee ~~(13)~~ and at said server ~~(12)~~.

17. (currently amended) A method according to claim 16, wherein said cryptographic parameters ~~(K(ID),A(ID))~~ associated to said delegatee ~~(13)~~ are generated by the respective delegator ~~(11)~~ and provided to said delegatee ~~(13)~~ and to said server ~~(12)~~.

18. (currently amended) A method according to claim 1, wherein said delegator ~~(11)~~ forwards said piece of information to a slave device ~~(13,33)~~ only in case said delegator ~~(11)~~ determines that said slave device ~~(13,33)~~ comprises a tamper resistant certificate indicating that said slave device ~~(13,33)~~ is compliant with predetermined rights issuer rules.

19. (currently amended) A method according to claim 1, wherein said delegator ~~(11)~~ forwards said second part of said secret master key to said server ~~(12)~~ only in case said delegator ~~(11)~~ determines that said server ~~(12)~~ comprises a tamper resistant certificate indicating that said server ~~(12)~~ is compliant with predetermined rights issuer rules.

20. (currently amended) A method according to claim 1, wherein a delegatee ~~(13,23)~~ makes use of a delegated authorization by transmitting a request to perform a partial secret key operation on an included message ~~(m)~~ to said server ~~(12)~~, said server ~~(12)~~ performing a partial secret key operation on said

received message ~~(m)~~ based on a respective second part ~~(d_2,d_{24})~~ of said secret master key ~~(d)~~ and transmitting a resulting message as response message to said delegatee ~~(13,23)~~, and wherein said delegatee ~~(13,23)~~ performs a partial secret key operation on said transmitted message ~~(m)~~ based on said computed first part ~~(d_1,d_{11})~~ of said secret master key ~~(d)~~ and combines a resulting message with said response message received from said server ~~(12)~~.

21. (currently amended) A method according to claim 20, wherein a delegator ~~(11,13)~~ transmits to said server ~~(12)~~ a password verification value ~~(b)~~ provided by a respective delegatee ~~(13,23)~~ to said delegator ~~(11,13)~~ during the delegation of said authorization, which password verification value ~~(b)~~ is generated by said delegatee ~~(13,23)~~ based on a password entered by a user ~~(15)~~ of said delegatee ~~(13,23)~~ and on a random number, wherein said delegatee ~~(13,23)~~ transmits to said server ~~(12)~~ together with each request to perform a partial secret key operation on a message ~~(m)~~ a password verification value ~~(□)~~ generated by said delegatee ~~(13,23)~~ based on a password entered by a user ~~(15)~~ of said delegatee ~~(13,23)~~ for the respective request and on said random number, and wherein said server ~~(12)~~ verifies the identity of a user ~~(15)~~ using said delegatee ~~(13,23)~~ before performing said requested partial secret key operation by comparing said password verification values ~~(b,□)~~ received from said delegator ~~(11,13)~~ and from said delegatee ~~(13,23)~~.

22. (currently amended) A method according to claim 20, wherein said server ~~(12)~~ verifies the identity of a delegatee ~~(13,23)~~ requesting a partial secret key operation on a message ~~(m)~~ before performing a requested partial secret key operation on a received message ~~(m)~~.

23. (currently amended) A method according to claim 20, wherein said delegator ~~(11)~~ transmits a voucher to said delegatee ~~(13,33)~~ to which it forwards said piece of information, said voucher indicating an extent of a right of said

delegator to share said authorization, wherein a delegatee ~~(13)~~ includes in a request transmitted to said server ~~(12)~~ to perform a partial secret key operation an indication of said right of said delegator ~~(11)~~ to share said authorization received in said voucher, and wherein said server ~~(12)~~ performs a partial secret key operation on a message received in a request by a delegatee ~~(13)~~ only in case it determines that said request by said delegatee ~~(13)~~ is covered by said indicated extend of said right of said delegator ~~(11)~~ to share said authorization.

24. (original) A method according to claim 23, wherein said indication in said voucher comprises the number of devices allowed to make use of a specific content, for which said requested partial secret key operation is required, at the same time.

25. (currently amended) A delegator ~~(11,13) comprising~~
- configured to generate a first part and a second part of an available predetermined secret master key, said first part and said second part being combinable to said secret master key, wherein resources are accessible via messages on which a secret key operation was applied with said secret master key, and wherein said delegator is a delegator of an authorization to use said specific resources;
- configured to forward a piece of information to a slave device acting as a delegatee of said authorization, which piece of information enables said slave device to perform a partial secret key operation on messages based on said first part of said secret master key; and
- configured to forward said second part of said secret master key to a server for enabling said server to perform a partial secret key operation on messages received from said slave device based on said second part of said secret master key.

~~means for delegating an authorization to use specific resources to a delegatee (13,23,33) according to claim 1.~~

26. (currently amended) A delegatee ~~(13,23,33) comprising~~

- configured to ~~means for~~ request~~ing~~ an authorization to use specific resources from a delegator, wherein said resources are accessible via messages on which a secret key operation is applied with a predetermined secret master key available at said delegator;
- configured to ~~and~~ receive ~~ing an authorization to use specific resources~~ from said ~~a~~ delegator a piece of information,
- configured to use said piece of information to perform a partial secret key operation on messages based on a first part of said secret master key; and
- configured to co-operate with a server which is configured to perform a partial secret key operation on messages based on a second part of said secret master key, wherein said first part and said second part of said secret master key are combinable to said secret master key~~(11,13) according to claim 1~~.

27. (currently amended) A server ~~(12) comprising means for supporting a chained delegation of an authorization to use specific resources from a respective delegator (11,13) to a respective delegatee (13,23) according to claim 2.~~

- configured to receive from a delegator a second part of a secret master key, said second part being combinable with a first part of said secret master key available at a delegatee, wherein resources are accessible via messages on which a secret key operation was applied with said secret master key,
- configured to receive from said delegatee a second part of said first part of said secret master key, said second part of said first part of said secret master key being combinable with a first part of said first part of said secret master key available at a second delegatee to said first part of said secret master key; and
- configured to combine said second part of said secret master key with said second part of said first part of said secret master key to obtain a further second part of said secret master key for enabling said server to perform a

partial secret key operation on messages received from said second delegatee based on said further second part of said secret master key.

28. (new) A method comprising:
- requesting an authorization to use specific resources from a delegator, wherein said resources are accessible via messages on which a secret key operation is applied with a predetermined secret master key available at said delegator;
- receiving from said delegator a piece of information,
- using said piece of information to perform a partial secret key operation on messages based on a first part of said secret master key; and
- co-operating with a server which is configured to perform a partial secret key operation on messages based on a second part of said secret master key, wherein said first part and said second part of said secret master key are combinable to said secret master key.

29. (new) A method comprising:
- receiving from a delegator a second part of a secret master key, said second part being combinable with a first part of said secret master key available at a delegatee, wherein resources are accessible via messages on which a secret key operation was applied with said secret master key,
- receiving from said delegatee a second part of said first part of said secret master key, said second part of said first part of said secret master key being combinable with a first part of said first part of said secret master key available at a second delegatee to said first part of said secret master key; and
- combining said second part of said secret master key with said second part of said first part of said secret master key to obtain a further second part of said secret master key for being enabled to perform a partial secret key operation on messages received from said second delegatee based on said further second part of said secret master key.

30. (new) An apparatus comprising:
    - means for generating a first part and a second part of an available predetermined secret master key, said first part and said second part being combinable to said secret master key, wherein resources are accessible via messages on which a secret key operation was applied with said secret master key, and wherein said apparatus is a delegator of an authorization to use said specific resources;
    - means for forwarding a piece of information to a slave device acting as a delegatee of said authorization, which piece of information enables said slave device to perform a partial secret key operation on messages based on said first part of said secret master key; and
    - means for forwarding said second part of said secret master key to a server for enabling said server to perform a partial secret key operation on messages received from said slave device based on said second part of said secret master key.

31. (new) An apparatus comprising:
    - means for requesting an authorization to use specific resources from a delegator, wherein said resources are accessible via messages on which a secret key operation is applied with a predetermined secret master key available at said delegator;
    - means for receiving from said delegator a piece of information,
    - means for using said piece of information to perform a partial secret key operation on messages based on a first part of said secret master key; and
    - means for co-operating with a server which is configured to perform a partial secret key operation on messages based on a second part of said secret master key, wherein said first part and said second part of said secret master key are combinable to said secret master key.